IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

SPECIAL SECTION ON SECURITY AND PRIVACY FOR VEHICULAR NETWORKS

Received April 25, 2018, accepted May 21, 2018, date of publication May 28, 2018, date of current version July 25, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2841008

PAAS: PMIPv6 Access Authentication Scheme Based on Identity-Based Signature in VANETs

TIANHAN GAO[1], XINYANG DENG[1], YINGBO WANG[1], AND XIANGJIE KONG[2], (Senior Member, IEEE)

[1]Software College, Northeastern University, Shenyang 110169, China
[2]School of Software Technology, Dalian University of Technology, Dalian 116024, China

Corresponding authors: Xinyang Deng (xinyang1121@sina.com) and Xiangjie Kong (xjkong@ieee.org)

This work was supported in part by the National Natural Science Foundation of China under Grants 61402095 and 61300196, and in part by the China Fundamental Research Funds for the Central Universities under Grants N120404010, N130817002, and DUT18JC09.

ABSTRACT Due to the advantages of low handover latency and signaling costs, Proxy Mobile IPv6 (PMIPv6), as a localized mobility management protocol for next generation mobile network, can be well combined with vehicular ad-hoc networks. However, the lack of security considerations limits the rapid growth of PMIPv6. Unfortunately, few proposals are in the literature to address such issue. Motivated by this, a novel authentication scheme based on identity-based signature for PMIPv6 is proposed. Mutual authentication between mobile node and mobile access gateway is achieved for both intra-domain and inter-domain scenarios with the help of identity-based signature and service-level agreement. The authentication signaling can be finely integrated into the mobility management procedure of PMIPv6, which equips our scheme with high authentication efficiency. The formal security proof under SVO logic and the performance analysis are presented to demonstrate the robustness and efficiency of our proposed scheme.

INDEX TERMS VANETs, PMIPv6, mutual authentication, identity-based signature, SVO.

I. INTRODUCTION

The rapid development of transportation and wireless network has greatly promoted the popularization of vehicular ad-hoc networks(VANETs). MIPv6 protocol [4], which allows mobile node to be online regardless of its movement and location, is an ideal protocol applied to vehicular ad-hoc networks [5]. However, MIPv6 also faces many problems such as security, efficiency, package loss. Therefore, several enhanced schemes are introduced including HMIPv6 [6], FMIPv6 [7], and PMIPv6 [13], where PMIPv6 has the lowest handover delay and configuration requirement that gains more attentions from researchers and practitioners consequently.

Reliable wireless communication is essential demands for VANETs [14], without safety, it is impossible for PMIPv6 to be widely adopted as a network-based mobility management protocol in VANETs. According to [15], [16], there are various attacks including stolen-verified, denial of service, impersonation, replay, password guessing, as well as man-in-the-middle attack, which threat the PMIPv6 network seriously. It is worth to note that RFC5213, a specification for PMIPv6, doesn't provide details for authentication and other security concerns.

To the end, experts proposed some security scheme for PMIPv6. Zhang *et al.* [17] present an authentication scheme based on certificateless signcryption, and the use of signcryption scheme ensures the confidentiality, reliability during message interaction process. Zhang and Wuhan [18] utilize the improved scheme of IBC to realize the secure handover of MN, which can solve the key escrow problem effectively. Reference [19] is a Diameter based on PMIPv6 authentication scheme. During authentication process, each entity implements authentication by using sharedkey with the AAA server and guarantees the security of the key. However, in [17]–[19], MNs need to be authenticated by their home authentication server(AS), which causes much burden for the home AS. In order to solve these problems, Kim and Lee [20] propose an authentication scheme, which is based on the Diffie-Hellman key. However, this scheme suffers from the latency of session key generations, which clearly influences the

handover efficiency. On the other hand, SPAM [21] presents a secure password authentication mechanism by using smart card to store relevant information, which has the advantage in terms of security and efficiency. But, from [22], [23], we can see that SPAM still has critical security flaws. HOTA [34] proposes a ticked based on authentication scheme. Using the same credential issued by AS, no matter where MN is located, HOTA can achieve authentication. However, during initial authentication, the credential has to be ensured by AS which increases transmission overhead.

In this paper, we propose a PMIPv6 access authentication scheme based on identity-based signature in VANETs. Mutual authentication between MN and MAG is achieved for initial authentication without knowing the other party's identity. At the same time, the design of hierarchical architecture decreases the pressure of System-level Trust Root (STR) and Local Mobility Anchor (LMA), shortens MN's waiting time and improves the whole authentication efficiency. The formal security proof under SVO logic and the performance analysis show that the proposed scheme can maintain a balance between efficiency and security well.

The rest of this paper is organized in the following manner. The related theory and cryptography building blocks are reviewed in Section 2. The proposed scheme is established in Section 3. The security and performance analysis are given in Section 4, and Section 5 respectively. Finally, we get a conclusion in Section 6.

II. PRELIMINARIES

A. VANETs

As shown in Figure 1, VANETs is a special mobile ad hoc networks(MANETs) which can guarantee the Vehicle-to-vehicle(V2V) communications, and Vehicle-to-Infrastructure(V2I) communications. Due to the device equipped with computing capabilities, positioning, communicating, etc., the vehicle has the ability to sense its own driving data, perform message broadcasting and forwarding to neighboring nodes. RSU is seen as a gateway to connect internet and vehicles, each vehicle can obtain internet services through RSU. As the part of the intelligent transportation system(ITS) in Smart Cities [8], vehicle can avoid congested road, ensure the security of driving through message broadcasting and forwarding. Meanwhile, RSU can collect vehicle status information, obtain traffic status of the road, and assist in supervising road conditions [9]. Beside, by combining with the socially aware networking and Internet of Things, VANETs can also provide diverse application services for drivers [9]–[12].

B. PMIPv6

In 2008, PMIPv6 was proposed as a network-based mobility management protocol [13]. PMIPv6 introduces two new entities, Local Mobility Anchor (LMA) and Mobile Access Gateway (MAG). In Figure.2, MAG executes on an access router and is responsible for tracking MN's mobility status,

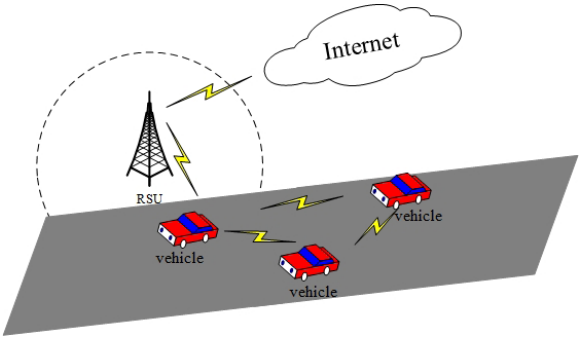


FIGURE 1. Network architecture of VANETs.

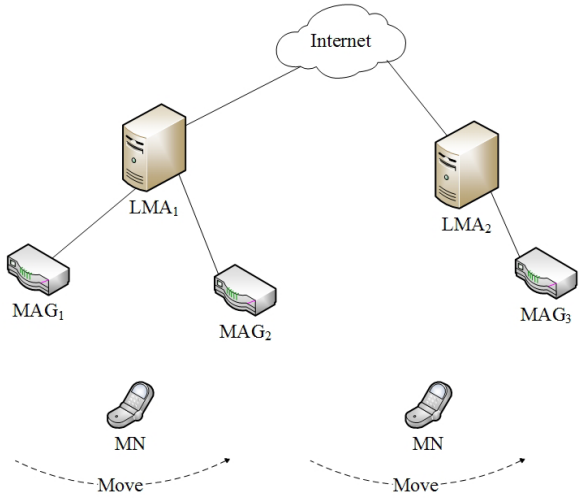


FIGURE 2. Network architecture of PMIPv6.

handling the mobility-management signaling on behalf of MN, which decreases the complexity of MN's protocol stack. LMA, acting as a home agent of MN, is responsible for managing binding status of MN and establish the bi-directional tunnel to forward packages.

The whole access process of MN contains initial access phrase and handover access phrase. The initial access phrase is that MN conducts the binding registration of PMIPv6 when entering the PMIPv6 domain firstly. The handover access authentication is that MN changes its access point or user interface when roaming in the PMIPv6 domain. In initial access phrase, when MAG detects MN's access, it can obtain MN's configuration files which contains user's ID, service provider's ID, and LMA's address. Then, MAG sends Proxy Binding Update (PBU) to LMA on behalf of MN. After receiving the PBU, LMA sends Proxy Binding Acknowledgement (PBA) with MN's home network prefix to MAG and establishes a bi-directional tunnel with MAG. Meanwhile, LMA also establishes a binding cache entry (BCE) to store MN's relevant registration information. After receiving PBA, MAG sends Router Advertisement (RA) to MN and informs MN its Home Network Prefix (HNP). MN is then able to configure its formal IPv6 address using the HNP and obtain the

network service through the bi-directional tunnel. During the handover access phase, when MN changes its access point, the previous MAG (pMAG) can detect MN's departure. At the same time, pMAG sends PBU to LMA for cancelling MN's binding status. LMA replies PBA to pMAG and releases the bi-directional tunnel between pMAG and LMA. Afterwards, MN is able to access to the new MAG (nMAG) with the same manner of initial access phrase.

C. BILINEAR PAIRING

Let G_1 be a cyclic additive group generated by P, whose order is a prime q, and G_T be a multiplicative group of the same prime order. I_{G_T} is the generator of G_T. Assume that the discrete logarithm problem [25] is hard on both G_1 and G_T. A bilinear pairing e: $G_1 \times G_1 \rightarrow G_T$ owns the following properties:

1) Bilinear: For all $P, Q \in G_1$ and $a, b \in Z_q^*$, $e(aP, bQ) = e(P, Q)^{ab}$, where $Z_q^* = \{1, 2, \ldots q-1\}$;
2) Non-degenerate: There exists $P, Q \in G_1$ such that $e(P, Q) \neq I_{G_T}$;
3) Computable: For all $P, Q \in G_1$, there is an efficient method to compute $e(P, Q)$.

D. WU's IDENTITY-BASED SIGNATURE SCHEME

In 2007, Wu *et al.* [25] put forward an efficient identity-based signature scheme(WMS) holding the security proof under the random oracle model. The scheme contains ParaGen, KeyExtract, StandardSign, StandardVerify algorithms.

- WMS.ParaGen — Input the system parameter l, the private key generators(PKG) generates a bilinear group G_1 of prime order q, bilinear pairing e: $G_1 \times G_1 \rightarrow G_T$, where G_T is a multiplicative group of the same prime order q, a generator P of G_1. PKG selects a master key $s \in Z_q^*$ randomly and computes $P_{Pub} = sP$ as the public key. At the same time, PKG chooses two different secure hash functions H_0, H_1: $\{0,1\}^* \rightarrow G_1$. The system public parameters are $\{G_1, G_T, q, e, P, P_{Pub}, H_0, H_1\}$.
- WMS.KeyExtract — For the given string $ID \in \{0,1\}^*$, PKG generates the user private key $sk_{ID} = sH_0(ID)$.
- WMS.StandardSign — In order to sign message $M \in \{0,1\}^*$, the signer selects $r \in Z_q^*$, and signs M as: $Sign=(\delta_1, \delta_2)$, $\delta_1 = sk_{ID} + rH_1(M)$, $\delta_2 = rP$.
- WMS.StandardVerify — In order to verify the signature $Sign$, the verifier checks whether $e(\delta_1, P) == e(H_0(ID), P_{pub})e(H_1(M), \delta_2)$ holds. If the equation holds, the signature is valid, otherwise, the signature is invalid.

III. THE PROPOSED SCHEME

A. HIERARCHICAL NETWORK ARCHITECTURE

In this section, we provide a scenarios that VANETs and PMIPv6 are combined. As depicted in Figure 3, The first layer is the System-level Trusted Root (STR) that is trusted by all entities, is in charge of issuing the private key for other entities. The second layer includes several LMAs. As an auxiliary entity of VANETs, LMA is responsible for managing binding status of MN and establishes the bi-directional tunnel to forward packages. Besides, LMA also provides registration and authentication service for MAGs. The third layer contains MAGs which is integrated with RSU and is deployed on both sides of the road to provide authentication, security communications and other related services for MN. The forth layer is formed by MNs, which refer to vehicle nodes. MN can rely on the infrastructure deployed on the roadside to access the network and communicate, besides, during driving, MN can switch from one network or subnet to another, and ensure the stability of the communication.

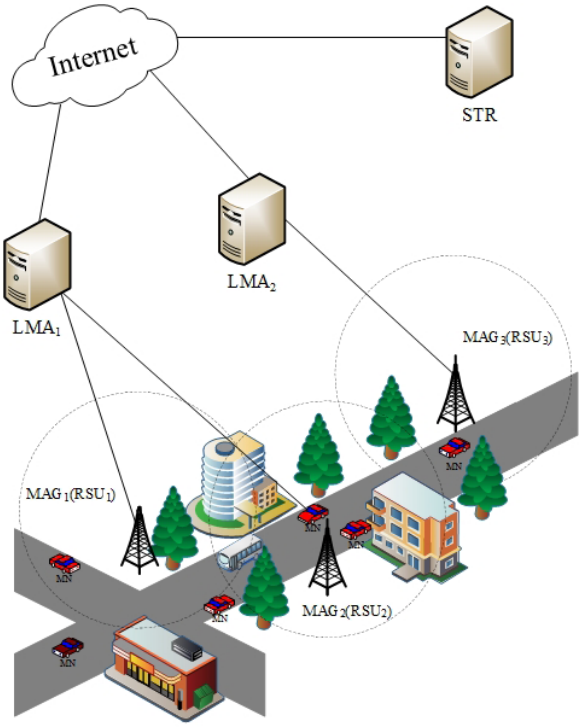


FIGURE 3. Hierarchical network architecture.

B. TRUST MODEL AND ASSUMPTIONS

The trust model is shown as Figure.4.

1) As the system-trusted root, STR is absolutely credible. All the entities trust the public key of STR.
2) MAGs in the same LMA domain trust each other depending on the pre-established secure tunnel. MAGs in different LMA domains have no trust relationship.
3) LMAs can establish trust relationship by signing service-level agreement(SLA) to trust the other party's public key.
4) Before performing the access authentication, MAG and MN have no trust relationship.

Generally, TA, LMA, and MAG are difficult to be compromised and if MN is compromised, the communication among entities has not been greatly affected. Thus we assume a global passive attacker existed who owns the common attack capabilities, such as impersonation, replay, etc.

TABLE 1. Relevant identifier.

Notation	Description
ID_A	The identity of entity A
PK_A/SK_A	Public / Private key of entity A
$PEnc\_ALG\_PK_A\{M\}$	Using entity A's PK_A to encrypt message M through ALG mechanism
$Sign\_ALG\_SK_A\{M\}$	Using entity A's SK_A to sign message M through ALG mechanism
K_{A-B}	The shared key between entity A and entity B
$SE_{K_{A-B}}\{M\}$	Encrypt message M using K_{A-B}
TS	The current time stamp
$M_1 \| M_2$	Concatenation of message and M_1 and M_2
SEK_{A-B}	Session key between entity A and entity B

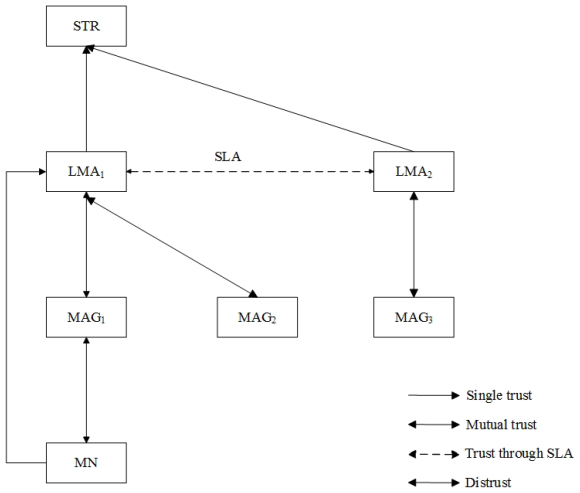


FIGURE 4. Trust model.

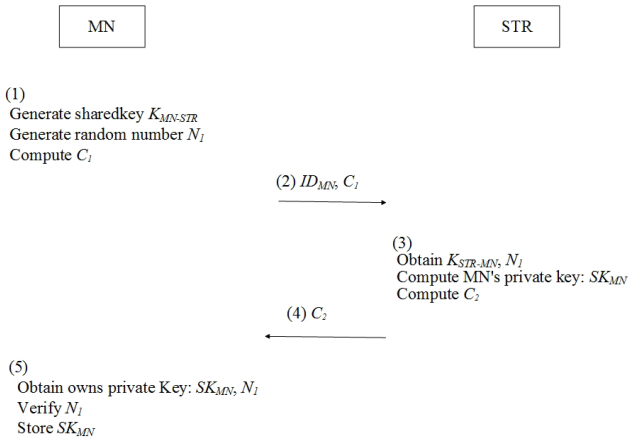


FIGURE 5. MN's registration process.

C. THE ACCESS AUTHENTICATION SCHEME

The proposed PMIPv6 access authentication scheme in vehicular scenarios(PAAS) is composed of four phrases: registration, initial access authentication, intra-domain handover authentication, and inter-domain handover authentication.

For the convenience of the later description, the relevant notations and descriptions are shown as Table 1.

1) REGISTRATION

Before registration, STR generates a bilinear group G_1 of prime order q, a bilinear pairing e:$G_1 \times G_1 \rightarrow G_T$, where G_1 is a multiplicative group of the same prime order q, and a generator P of G_1. STR selects a master key $SK_{STR} \in Z_q^*$ randomly and computes its public key $PK_{STR} = SK_{STR}P$. At the same time, STR selects three secure hash functions H: $\{0,1\}^* \rightarrow \{0,1\}^l$, H_0, H_1:$\{0,1\}^* \rightarrow G_1$, where l is the length of the session key. The system public parameters are $\{G_1, G_T, q, e, P, P_{pub}, H, H_0, H_1\}$.

a: MN's REGISTRATION

As shown in Figure.5, MN's registration process is composed of the following steps.

(1) MN generates the shared key $K_{MN-STR} \in \{0,1\}^*$ and random number $N_1 \in Z_q^*$. MN uses PK_{STR} to encrypt K_{MN-STR}, N_1 and gets the ciphertext $C_1 = Enc\_IBE\_PK_{STR}\{K_{MN-STR}, N_1\}$. The encryption algorithm here can be any identity-based encryption algorithm such as BF-IBE [26], Waters [27], etc

(2) MN sends ID_{MN} and C_1 to STR for registration.

(3) STR uses SK_{STR} to decrypt C_1 and obtains K_{MN-STR}, N_1. STR generates the private key of MN $SK_{MN} = S_{STR}H_0(ID_{MN})$ and encrypt SK_{MN}, N_1 to get the ciphertext $C_2 = \text{SE}_{K_{STR-MN}}\{SK_{MN}, N_1\}$.

(4) STR sends C_2 to MN.

(5) MN uses K_{MN-STR} to decrypt C_2 and gets SK_{MN}, N_1. MN verifies N_1, if N_1 is valid, then MN preserves SK_{MN}. Otherwise, the registration is failed.

b: MAG AND LMA's REGISTRATION

(1) Each MAG$_i$ in the same LMA domain chooses $S_{MAG_i} \in Z_q^*$ and computes $M_{MAG_i} = S_{MAG_i}H_0(ID_{MAG_i})$.

(2) For the convenience of registration, MAG$_i$ sends M_{MAG_i} and ID_{MAG_i} to LMA.

(3) After receiving the message from MAG$_i$, LMA selects the shared key $K_{LMA-STR}$, $N_2 \in Z_q^*$, and uses PK_{STR} to encrypt $K_{LMA-STR}$, N_2 to get the ciphertext $C_3 = Enc\_IBE\_PK_{STR}\{K_{LMA-STR}, N_2\}$.

(4) LMA sends ID_{MAG_i}, ID_{LMA}, C_3, and M_{MAG_i} to STR.

(5) STR uses its private key SK_{STR} to decrypt C_3 and obtain $K_{STR-LMA}$ and N_2. Then STR generates $S_i = S_{STR}M_{MAG_i}$ and

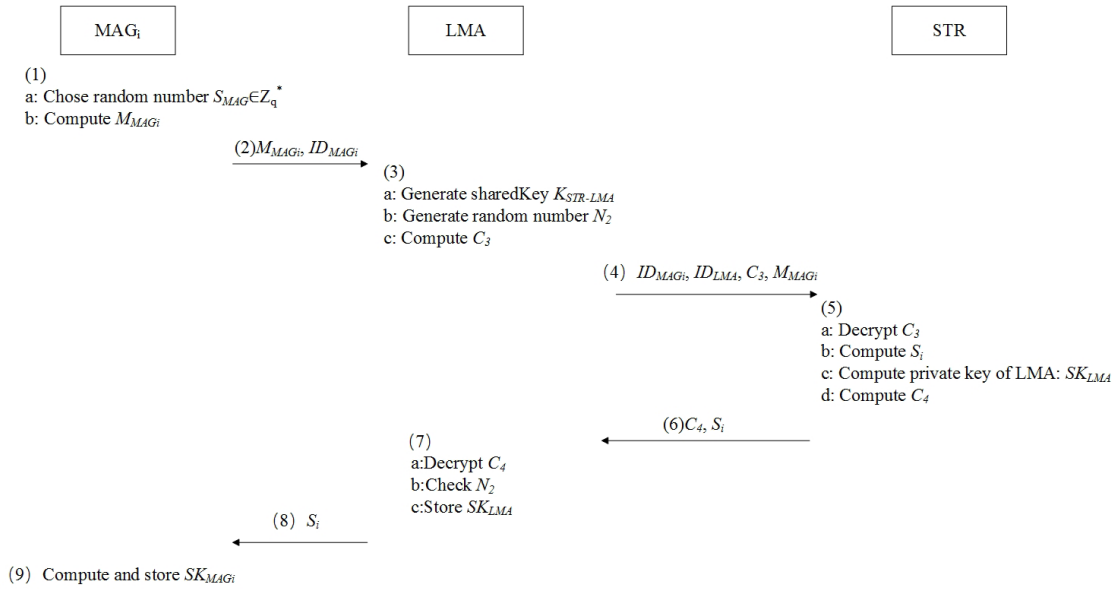


FIGURE 6. MAG and LMA's registration process.

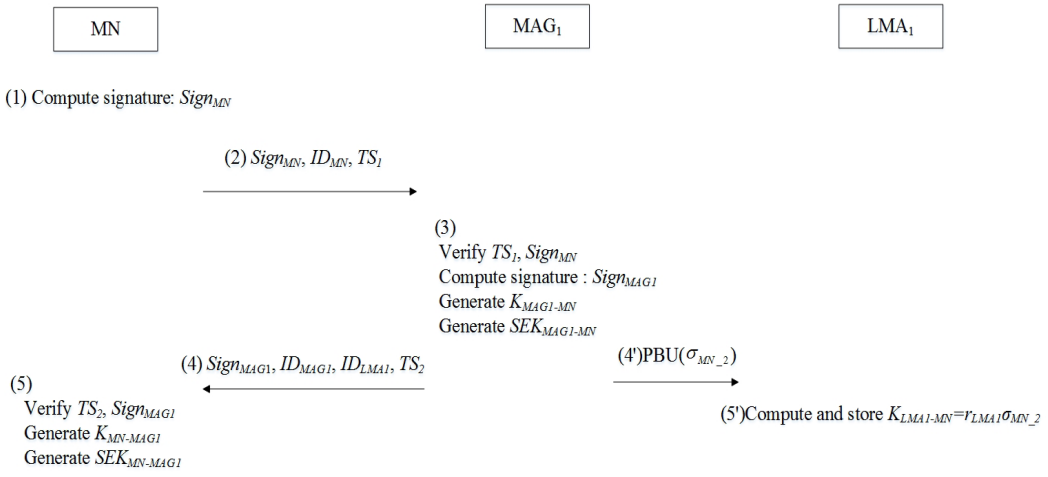


FIGURE 7. The workflow of initial authentication protocol.

LMA's private key $SK_{LMA} = S_{STR}H_0(ID_{LMA})$. Finally, STR uses $K_{STR-LMA}$ to encrypt SK_{LMA}, N_2 and gets the ciphertext $C_4 = SE_{K_{LMA-STR}}\{SK_{LMA}, N_2\}$.

(6) STR sends C_4, S_i to LMA.

(7) After receiving C_4 and S_i, LMA decrypts C_4 to obtain SK_{LMA}, N_2. Then LMA checks N_2, if N_2 is valid, LMA preserves SK_{LMA}. Otherwise LMA discards the received message.

(8) LMA forwards S_i to each MAG$_i$.

(9) After receiving S_i, MAG$_i$ gets its own private key $SK_{MAG_i} = S_i S_{MAG_i}^{-1}$.

2) INITIAL AUTHENTICATION PROTOCOL

The initial authentication protocol works when MN first attaches a PMIPv6 domain and launches mutual authentication with the accessed MAG. The detail of initial authentication protocol is shown as Figure.7 in terms of the scenario in Figure.3.

(1) MN chooses r_{MN} randomly. Through using SK_{MN}, MN signs ID_{MN}, TS_1, and obtains $Sign_{MN} = Sign\_WMS\_SK_{MN}\{ID_{MN}, TS_1\} = (\sigma_{MN\_1}, \sigma_{MN\_2})$, where $\sigma_{MN\_1} = SK_{MN} + r_{MN}H_1(ID_{MN}||TS_1)$, $\sigma_{MN\_2} = r_{MN}P$, $r_{MN} \in Z_q^*$.

(2) MN sends ID_{MN}, TS_1, $Sign_{MN}$ to MAG$_1$.

(3) After receiving the message from MN, MAG$_1$ first checks the freshness of TS_1. If not, the authentication is failed. Otherwise MAG$_1$ verifies the signature $Sign_{MN}$. If the verification failed, then MN is not a legal node and the authentication is failed. Otherwise, MAG$_1$ makes sure that MN is a legal node. MAG$_1$ selects random number $r_{MAG_1} \in Z_q^*$, and generates $Sign_{MAG_1} = Sign\_WMS\_SK_{MAG_1}\{ID_{MAG_1}, ID_{LMA_1}, TS_2\} = \{\sigma_{MAG_1\_1}, \sigma_{MAG_1\_2}\}$, where $\sigma_{MAG_1\_1} = SK_{MAG_1} + r_{MAG_1}H_1(ID_{MAG_1}||ID_{LMA_1}||TS_2)$, $\sigma_{MAG_1\_2} = r_{MAG_1}P$.

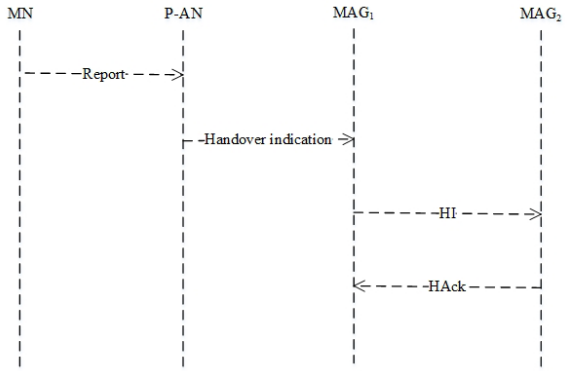


FIGURE 8. FPMIPv6 operations.

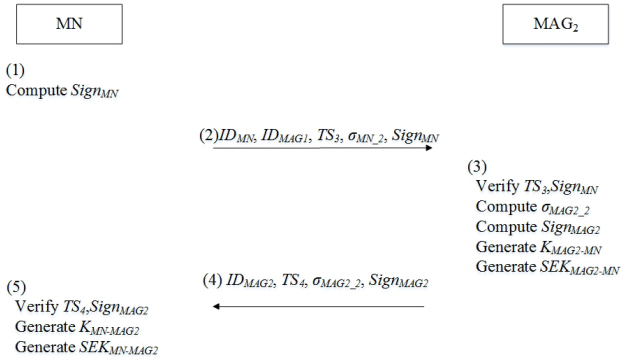


FIGURE 9. The workflow of intra-domain handover authentication protocol.

Finally, MAG_1 generates the shared key and session key: $K_{MAG_1-MN} = r_{MAG_1}\sigma_{MN\_2}$, $SEK_{MAG_1-MN} = H(K_{MAG_1-MN}||TS_1||TS_2)$.

(4) MAG_1 sends ID_{MAG_1}, ID_{LMA_1}, TS_2, and $Sign_{MAG_1}$ to MN.

(4') MAG_1 sends σ_{MN_2} through PBU to LMA_1.

(5') After getting σ_{MN_2}, LMA_1 computes and preserves the shared key: $K_{LMA_1-MN} = r_{LMA_1}\sigma_{MN\_2}$.

(5) After receiving the message from MAG_1, MN first checks whether TS_2 is fresh, if not, the authentication is failed. Otherwise, MN verifies $Sign_{MAG_1}$, if $Sign_{MAG_1}$ is invalid, MAG_1 is unreliable and the authentication is failed. Otherwise, MAG_1 is regarded as a reliable node. MN generates the shared key and the session key: $K_{MN-MAG_1} = r_{MN}\sigma_{MAG_1\_2}$, $SEK_{MN-MAG_1} = H(K_{MN-MAG_1}||TS_1||TS_2)$.

D. INTRA-DOMAIN HANDOVER AUTHENTICATION PROTOCOL

Intra-domain handover take place when MN detaches from the previous MAG(MAG_1) and is ready to attach the new MAG(MAG_2) in the same LMA domain as shown in Figure3. According to the FPMIPv6 protocol [28], MN has the ability to report the link layer information to the Access Network (AN). Afterwards, AN relays the handover indication to MAG_1. In Figure.8, when MN detects that a handover is imminent, it forwards ID_{MN} and New Access Point Identifier ID_{n-AP} [7] to MAG_1 through the current connected access network p-AN. According to ID_{n-AP}, MAG_1 is able to detect MAG_2. MAG_1 then sends the Handover Initiate(HI) which contains ID_{MN}, ID_{MAG_1}, and the shared key $K_{MAG_1-MN}$to MAG_2. After receiving HI from MAG_1, MAG_2 confirms that they are in the same LMA domain. MAG_2 preserves ID_{MN}, ID_{MAG_1}, K_{MAG_1-MN} and sends the Handover Acknowledgement(HAck) to MAG_1.

When MN is ready to attach the new MAG (MAG_2), the Intra-domain handover authentication process between MN and MAG_2 is shown as Figure.9.

(1) MN derives the signature $Sign_{MN} = Sign\_HMAC\_K_{MN-MAG_1}\{ID_{MN}, ID_{MAG_1}, TS_3, \sigma_{MN\_2}\} = H(ID_{MN}||ID_{MAG_1}||TS_3||\sigma_{MN\_2}||K_{MN-MAG_1})$, where $\sigma_{MN\_2} = r_{MN}P$.

(2) MN sends ID_{MN}, ID_{MAG_1}, TS_3, σ_{MN_2}, and $Sign_{MN}$ to MAG_2.

(3) After receiving the message from MN, MAG_2 first checks the freshness of TS_3, if TS_3 is not fresh, then the authentication failed. Otherwise, MAG_2 verifies $Sign_{MN}$ and if it is invalid, the process stop. Othewise,, MAG_2 signs ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$ with K_{MAG_1-MN} and gets the signature $Sign_{MAG_2} = Sign\_HMAC\_K_{MAG_1-MN}\{ID_{M-}\_AG_2, TS_4, \sigma_{MAG_2\_2}\} = H(ID_{MAG_2}||TS_4||\sigma_{MAG_2\_2}||K_{MAG_1-MN})$, where $\sigma_{MAG_2\_2} = r_{MAG_2}P$. Finally, MAG_2 generates the shared key and the session key: $K_{MAG_2-MN} = r_{MAG_2}\sigma_{MN\_2}$, $SEK_{MAG_2-MN} = H(K_{MAG_2-MN}||TS_3||\ TS_4)$.

(4) MAG_2 sends ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$, and $Sign_{MAG_2}$ to MN.

(5) After receiving the message from MAG_2, MN checks the freshness of TS_4 if TS_4 is not fresh, then the authentication failed. Othewise, MN continues to verify $Sign_{MAG_2}$ and if the verification is successful, MN will generate the shared key and the session key: $K_{MN-MAG_2} = r_{MN}\sigma_{MAG_2\_2}$, $SEK_{MN-MAG_2} = H(K_{MN-MAG_2}||TS_3||TS_4)$. Otherwise, the authentication failed and the authentication process stops.

E. INTER-DOMAIN HANDOVER AUTHENTICATION PROTOCOL

During Inter-domain handover, MN departs from MAG_2 to MAG_3 which locates in another LMA domain (LMA_2) as shown in Figure.3. The same as the Intra-domain handover authentication, MAG_2 sends HI which contains ID_{MN}, ID_{MAG_2}, ID_{LMA_1} to MAG_3. MAG_3 then sends ID_{MN}, ID_{MAG_3} ID_{LMA_1} to LMA_2 to get K_{LMA_1-MN}. After receiving the message from MAG_3, LMA_2 requests K_{LMA_1-MN} from LMA through the secure channel and forwards the shared key to MAG_3. Afterwards MAG_3 preserves the key and sends HAck to MAG_2.

When MN handovers from the previous MAG (MAG_2) to the new MAG (MAG_3). The Inter-domain handover process is shown as Figure.10.

(1) MN signs ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2} with K_{MN-LMA_1} to obtain $Sign_{MN} = Sign\_HMAC\_K_{LMA_1-MN}\{ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, \sigma_{MN\_2}\} = H(ID_{MN}||ID_{MAG_2}||ID_{LMA_1}||TS_5||\sigma_{MN\_2}||K_{MN-LMA_1})$.

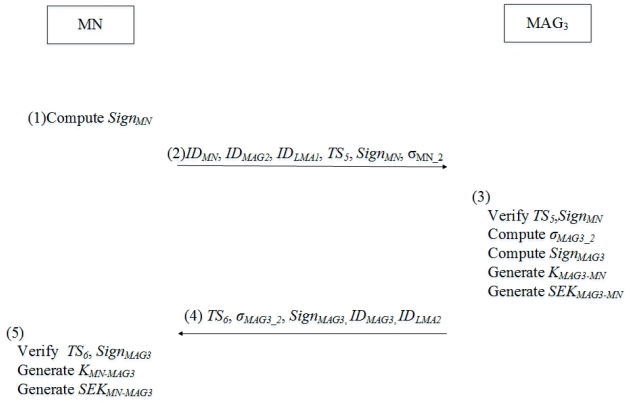


FIGURE 10. The workflow of inter-domain handover authentication protocol.

(2) MN sends ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN}, and $Sign_{MN}$ to MAG_3.

(3) After receiving the message from MN, MAG_3 checks the freshness of TS_5 and verifies the signature $Sign_{MN}$ through $ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, \sigma_{MN\_2}$, and K_{MN-LMA_1}. If either of the verifications is failed, then the process stops. If both of the verifications success, MAG_3 computes $Sign_{MAG_3} = H(ID_{MAG_3}||ID_{LMA_2}||TS_6||\sigma_{MAG_3\_2}||K_{LMA-MN})$, where $\sigma_{MAG_3\_2} = r_{MAG_3}P$. MAG_3 generates the shared key: $K_{MAG_3-MN} = r_{MAG_3}\sigma_{MN\_2}$ and the session key: $SEK_{MAG_3-MN} = H(K_{MAG_3-MN}||TS_5||TS_6)$.

(4) MAG_3 sends $ID_{MAG_3}, ID_{LMA_2}, TS_6, \sigma_{MAG_3\_2}, Sign_{MAG_3}$ to MN.

(5) After getting the message from MAG_3, MN first checks the freshness of TS_6, if it is not freshness, then the authentication failed. Otherwise, MN verifies $Sign_{MAG_3}$, if it is invalid, the process stops. Otherwise, MN finishes the mutual authentication and computes the shared key and the session key: $K_{MN-MAG_3} = r_{MN}\sigma_{MAG_3\_2}$, $SEK_{MN-MAG_3} = H(K_{MN-MAG_3}||TS_5||TS_6)$.

IV. SECURITY ANALYSIS OF THE PROPOSED SCHEME

In this section, we will provide formal security proof of the authentication protocols in PAAS through SVO Logic. Besides, the security analysis of PAAS from the aspects of mutual authentication, session key secrecy, reliability, as well as the resistance of man-in-middle attack will also be presented.

A. SVO LOGIC

SVO logic [29] is a security protocol analysis method proposed by Syverson and Orschot,which absorbs the advantages of BAN logic [30], GNY logic [31], AT logic [32], VO logic [33]. SVO logic has clear semantic, high expansion capability, and is easy to use.

SVO logic owns two basic inference rules and twenty axioms.

1) Inference rules:
   a) Modus Ponens(MP):$\varphi \wedge \varphi \supset \psi \Rightarrow \psi$.
   b) Necessitation (Nec): $\vdash \varphi \Rightarrow \vdash$P believe φ.
2) Axioms
   a) Believing
   Ax1: P believes $\varphi \wedge$ P believes $(\varphi \supset \psi) \supset P$ believes ψ
   Ax2: P believes $\varphi \supset$ P believes (P believes φ)
   b) Source Association
   Ax3: $SharedKey(K, P, Q) \wedge R$ received $\{X^Q\}_K \supset Q$ said $X \wedge Q$ sees K
   Ax4: $PK_\sigma(Q, K) \wedge R$ received $X \wedge SV(X, K, Y) \supset Q$ said Y
   c) Key Agreement
   Ax5: $PK_\delta(P, K_p) \wedge PK_\delta(Q, K_q) \supset SharedKey(F_0(K_p, K_q), P, Q)$
   Ax6: $\varphi \equiv \varphi[F_0(K, K')/F_0(K', K)]$
   d) Receiving
   Ax7: P received $(X_1, \cdots, X_n) \supset P$ received X_i
   Ax8: P received $\{X\}_K \wedge P$ sees $K^{-1} \supset P$ receives X
   Ax9: P received $[X]_K \supset P$ received X
   e) Seeing
   Ax10: P received $X \supset P$ sees X
   Ax11: P sees $(X_1, \cdots, X_n) \supset P$ sees X_i
   Ax12: P sees $X_1 \wedge \cdots \wedge P$ sees $X_n \subset P$ sees $F(X_1, \cdots, X_n)$
   f) Comprehending
   Ax13: P believes (P sees $F(X)$) $\supset P$ believes (P sees X)
   g) Saying
   Ax14: P said $(X_1, \cdots, X_n) \supset P$ said $X_i \wedge P$ sees X_i
   Ax15: P says $(X_1, \cdots, X_n) \supset P$ says $X_i \wedge P$ said $(X_1, \cdots, X_n)$
   h) Jurisdiction
   Ax16: P controls $\varphi \wedge P$ says $\varphi \supset \varphi$
   i) Freshness
   Ax17: $fresh(X_i) \supset fresh(X_1, \cdots, X_n)$
   Ax18: $fresh(X_1, \cdots, X_n) \supset (F(X_1, \cdots, X_n))$
   j) Nonce-Verification
   Ax19: $fresh(X) \wedge P$ said $X \supset P$ says X
   k) Symmetric goodness of shared keys
   Ax20: $SharedKey(K, P, Q) \equiv SharedKey(K, Q, P)$

B. FORMAL SECURITY PROOF OF THE AUTHENTICATION PROTOCOLS

1) Initial authentication protocol
   a) Assumptions
   P1: MN believes fresh(TS_2) MAG_1 believes fresh(TS_1)
   P2: MN believes MN received $(([ID_{MAG_1}, ID_{LMA_1}, TS_2]SK^{-1}_{MAG_1}, ID_{MAG_1}, ID_{LMA_1}, TS_2) \supset PK_\delta(\text{MAG}_1, \sigma_{MAG_1\_2}))$ MAG_1 believes MAG_1 received $(([ID_{MN}, TS_1]SK^{-1}_{MN}, ID_{MN}, TS_1) \supset PK_\delta(\text{MN}, \sigma_{MN\_2}))$

P3: MN believes $PK_\sigma(\mathrm{MAG}_1, PK_{MAG_1})$ MAG_1 believes $PK_\sigma(\mathrm{MN}, PK_{MN})$

P4: MN believes $\mathrm{SV}([ID_{MAG_1}, ID_{LMA_1}, TS_2]MSK^{-1}_{MAG_1}, PK_{MAG_1}, (ID_{MAG_1}, ID_{LMA_1}, TS_2))$ MAG_1 believes $\mathrm{SV}([ID_{MN}, TS_1]SK^{-1}_{MN}, PK_{MN}, (ID_{MN}, TS_1))$

P5: MN believes $PK_\delta(\mathrm{MN}, \sigma_{MN\_2})$ MAG_1 believes $PK_\delta(\mathrm{MAG}_1, \sigma_{MAG_1\_2}))$

P6: MN believes $((\mathrm{MAG}_1$ says $(ID_{MAG_1}, ID_{LMA_1}, TS_1) \supset PK_\delta(\mathrm{MAG}_1, \sigma_{MAG_1\_2}))$ MAG_1 believes $((\mathrm{MN}$ says $(ID_{MN}, TS_2) \supset PK_\delta(\mathrm{MN}, \sigma_{MN\_2}))$

P7: MN sees $PK_\delta(\mathrm{MN}, \sigma_{MN\_2})$ MAG_1 sees $PK_\delta(\mathrm{MAG}_1, \sigma_{MAG_1\_2})$

b) Goals

G_1: MAG_1 believes MN says (ID_{MN}, TS_1)

G'_1: MN believes MAG_1 says $(ID_{MAG_1}, ID_{LMA_1}$ $TS_2)$

G_2: MAG_1 believes SharedKey(K_{MAG_1-MN}-, MAG_1, MN)

G'_2: MN believes SharedKey(K_{MN-MAG_1}-, MN, MAG_1)

G_3: MAG_1 believes fresh(K_{MAG_1-MN})

G'_3: MN believes fresh(K_{MN-MAG_1})

c) Security proof According to Ax1, Nec:

S1: MAG_1 believes MAG_1 received $[ID_{MN}, TS_1]SK^{-1}_{MN}$

According to S1, P3, P4, Ax4:

S2: MAG_1 believes MN said (ID_{MN}, TS_1)

According to S2, P1, Ax19:

S3: MAG_1 believes MN says (ID_{MN}, TS_1) (G_1 **is proved)**

According to S3, P6, Ax1 and Nec:

S4: MAG_1 believes $PK_\delta(\mathrm{MN}, \sigma_{MN\_2})$

According to S4, P5, Ax5:

S5: MAG_1 believes SharedKey(K_{MAG_1-MN}, MAG_1, MN), K_{MAG_1-MN}=F($\sigma_{MAG_1\_2}, \sigma_{MN\_2}$)

According to P2, P7, Ax1, Ax5, Ax10:

S6: MAG_1 sees SharedKey(K_{MAG_1-MN}, MAG_1, MN), K_{MAG_1-MN}=F($\sigma_{MAG_1\_2}, \sigma_{MN\_2}$)

According to S5, S6, the definition of SharedKey (K-, A, B)

S7: MAG_1 believes SharedKey(K_{MAG_1-MN}, MAG_1, MN), K_{MAG_1-MN}=F($\sigma_{MAG_1\_2}, \sigma_{MN\_2}$) ($G_2$ **is proved)**

According to P1, P2, Ax1, Ax18 and MP:

S8: MAG_1 believes fresh(K_{MAG_1-MN}) (G_3 **is proved)**

According to Ax1, Nec:

S9: MN believes MN received $[ID_{MAG_1}, ID_{LMA_1}, TS_2]SK_{MAG_1^{-1}}$

According to S9, P3, P4, Ax4:

S10: MN believes MAG_1 said $(ID_{MAG_1}, ID_{LMA_1}, TS_2)$

According to S10, P1, Ax19:

S11: MN believes MAG_1 says $(ID_{MAG_1}, ID_{LMA_1}, TS_2)$ (G'_1 **is proved)**

According to S11, P6, Ax1 and Nec:

S12: MN_1 believes $PK_\delta(\mathrm{MAG}_1, \sigma_{MAG_1\_2})$

According to S12, P5, Ax5:

S13: MN believes SharedKey(K_{MN-MAG_1}, MN, MAG_1), $K_{MN-MAG_1} = F(\sigma_{MN\_2}, \sigma_{MAG_1\_2})$

According to P2, P7, Ax1, Ax5, Ax10:

S14: MN sees SharedKey(K_{MN-MAG_1}, MN, MAG_1), K_{MN-MAG_1}=F($\sigma_{MN\_2}, \sigma_{MAG_1\_2}$)

According to S13, S14, and the definition of SharedKey(K-, A, B) :

S15: MN believes SharedKey(K_{MN-MAG_1}-, MN, MAG_1), K_{MN-MAG_1}=F($\sigma_{MN\_2}, \sigma_{MAG_1\_2}$) ($G'_2$ **is proved)**

According to P1, P2, Ax1, Ax18 and MP:

S16: MN believes fresh (K_{MN-MAG_1}) (G'_3 **is proved)**

2) Intra-domain handover authentication protocol

a) Assumptions

P1: MN believes fresh(TS_4) MAG_1 believes fresh(TS_3)

P2: MN believes SharedKey(K_{MN-MAG_1}, MN, MAG_1) MAG_2 believes SharedKey (K_{MAG_1-MN}, MAG_1, MN)

P3: MN believes MN received $(([ID_{MAG_2}, TS_4, \sigma_{MAG_2\_2}]K_{MAG_1-MN}, ID_{MAG_2}, TS_4), \sigma_{MAG_2\_2} \supset PK_\delta(\mathrm{MAG}_2, \sigma_{MAG_2\_2}))$ MAG_2 believes MAG_2 received $([ID_{MN}, ID_{MAG_1} TS_3, \sigma_{MN\_2}]K_{MN-MAG_1}, ID_{MN}, ID_{MAG_1}, TS_3, \sigma_{MN\_2}) \supset PK_\delta(\mathrm{MN}, \sigma_{MN\_2}))$

P4: MN believes $PK_\delta(\mathrm{MN}, \sigma_{MN\_2})$ MAG_2 believes $PK_\delta(\mathrm{MAG}_2, PK_{MAG_2\_2}))$

P5: MN believes $((\mathrm{MAG}_2$ says $(ID_{MAG_2}, TS_4, \sigma_{MAG_2\_2})) \supset PK_\delta(\mathrm{MAG}_2, \sigma_{MAG_2\_2}))$ MAG_2 believes $((\mathrm{MN}$ says $(ID_{MN}, ID_{MAG_1} TS3, \sigma_{MN\_2})) \supset PK_\delta(\mathrm{MN}, \sigma_{MN\_2}))$

P6: MN sees $PK_\delta(\mathrm{MN}, \sigma_{MN\_2})$ MAG_2 sees $PK_\delta(\mathrm{MAG}_2, \sigma_{MAG_2\_2})$

b) Goals

G_4: MAG_2 believes MN says $(ID_{MN}, ID_{MAG_2}, TS_3, \sigma_{MN\_2})$

G'_4: MN believes MAG_2 says $(ID_{MAG_2}, TS_4, \sigma_{MAG_2\_2})$

G_5: MAG_2 believes SharedKey(K_{MAG_2-MN}-, MAG_2, MN)

G'_5: MN believes SharedKey(K_{MN-MAG_2}-, MN, MAG_2)

G_6: MAG_2 believes fresh(K_{MAG_2-MN})
G'_6: MN believes fresh(K_{MN-MAG_2})

c) Security proof

According to P3, Ax1:

S1: MAG_2 believes MAG_2 received [ID_{MN}, ID_{MAG_1}, TS_3, σ_{MN_2}]K_{MAG_1-MN}

According to S1, P2, Ax3:

S2: MAG_2 believes MN said (ID_{MN}, ID_{MAG_1}, TS_3, σ_{MN_2})

According to S2, P1, Ax17, Ax19:

S3: MAG_2 believes MAG_2 says (ID_{MN}, ID_{MAG_1}, TS_3, σ_{MN_2}) (G_4 **is proved**)

According to P5, S3, Ax1, Nec:

S4: MAG_2 believes PK_δ(MN, δ_{MN_2})

According to S4, P4, Ax5:

S5: MAG_2 believes SharedKey(K_{MAG_2-MN}, MAG_2, MN), K_{MAG_2-MN} = F($\delta_{MAG_2\_2}$, δ_{MN_2})

According to P3, Ax1, Ax10:

S6: MAG_2 believes MAG_2 sees PK_δ(MN, σ_{MN_2})

According to S6, P6, Ax11, Ax12:

S7: MAG_2 believes MAG_2 sees SharedKey (K_{MAG_2-MN}, MAG_2, MN), K_{MAG_2-MN} = F($\delta_{MAG_2\_2}$, δ_{MN_2})

According to S5, S6, and definition of SharedKey ($K-$, A, B)

S8: MAG_2 believes SharedKey(K_{MAG_2-MN}-, MAG_2, MN) (G_5 **is proved**)

According to S5, P1, Ax1, Ax18 and MP:

S9: MAG_2 believes fresh(K_{MAG_2-MN}) (G_6 **is proved**)

According to P3, Ax1:

S10: MN believes MN received [ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$]K_{MAG_1-MN}

According to S10, P2, Ax3:

S11: MN believes MAG_2 said (ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$)

According to S11, P1, Ax17, Ax19:

S12: MN believes MAG_2 says (ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$) (G'_4 **is proved**)

According to P5, S12, Ax1, and Nec:

S13: MN believes PK_δ(MAG_2, $\sigma_{MAG_2\_2}$)

According to S13, P4, Ax5:

S14: MN believes SharedKey(K_{MN-MAG_2}, MN, MAG_2), K_{MN-MAG_2}=F(σ_{MN_2}, $\sigma_{MAG_2\_2}$)

According to P3, Ax1, Ax10:

S15: MN believes MN sees PK_δ(MAG_2, $\sigma_{MAG_2\_2}$)

According to S15, P7, Ax11, Ax12:

S16: MN believes MN sees SharedKey(K_{MN-MAG_2}, MN, MAG_2), K_{MN-MAG_2} = F(σ_{MN_2}, $\sigma_{MAG_2\_2}$)

According to S14, S16 and definition of SharedKey(K-, A, B):

S17: MN believes MN SharedKey(K_{MN-MAG_2}-, MN, MAG_2) (G'_5 **is proved**)

According to S14, P1, Ax1, Ax18 and MP:

S18: MN believes fresh(K_{MN-MAG_2}) (G'_6 **is proved**)

3) Inter-domain handover authentication protocol

a) Assumptions

P1: MN believes fresh(TS_6) MAG_3 believes fresh(TS_5)

P2: MN believes SharedKey(K_{MN-LMA_1}, MN, LMA_1) MAG_3 believes SharedKey (K_{LMA_1-MN}, LMA_1, MN)

P3: MN believes MN received (([ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$]K_{MN-LMA_1}, ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$, TS_6) $\supset$ PK_δ(MAG_3, $\sigma_{MAG_3\_2}$)) MAG_3 believes (MAG_3 received ([ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2}] K_{LMA_1-MN}, ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2}) $\supset$ PK_δ(MN, σ_{MN_2}))

P4: MN believes PK_δ(MN, σ_{MN_2}) MAG_3 believes PK_δ(MAG_3, $PK_{MAG_3\_2}$))

P5: MN believes MAG_3 says (ID_{MAG_3}, ID_{LMA_2}, TS_6))$\supset$ PK_δ(MAG_3, $\sigma_{MAG_3\_2}$)) MAG_3 believes MN says (ID_{MN}, ID_{MAG_3}, ID_{LMA_1}, TS_5))$\supset$ PK_δ(MN,σ_{MN_2}))

b) Goals

G_7: MAG_3 believes MN says (ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2})
G'_7: MN believes MAG_3 says (ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$)
G_8: MAG_3 believes SharedKey(K_{MAG_3-MN}-, MAG_3, MN)
G'_8: MN believes SharedKey(K_{MN-MAG_3}-, MN, MAG_3)
G_9: MAG_3 believes fresh(K_{MAG_3-MN})
G'_9: MN believes fresh(K_{MN-MAG_3})

c) Security proof

According to P3, Ax1:

S1: MAG_3 believes MAG_3 received [ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2}]K_{LMA_1-MN}

According to S1, P2, Ax3:

S2: MAG_3 believes MN said(ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2})

According to S2, P1, Ax17, Ax19:

S3: MAG_3 believes MN says(ID_{MN}, ID_{MAG_2}, ID_{LMA_1}, TS_5, σ_{MN_2}) (G_7 **is proved**)

According to P5, S3, Ax1, Nec:

S4: MAG_3 believes PK_δ(MN, σ_{MN_2})

According to S4, P4, Ax5:

S5: MAG_3 believes SharedKey(K_{MAG_3-MN}, MAG_3, MN), K_{MAG_3-MN}=F($\sigma_{MAG_3\_2}$, σ_{MN_2})

According to P3, Ax1, Ax10:

S6: MAG_3 believes MAG_3 sees PK_δ(MN, σ_{MN_2})

According to S6, P5, Ax11, Ax12:

S7: MAG_3 believes MAG_3 sees SharedKey (K_{MAG_3-MN}, MAG_3, MN), K_{MAG_3-MN} = F($\delta_{MAG_3\_2}$, δ_{MN_2})

According to S5, S6, Ax1, and definition of SharedKey(K-, A, B):

S8: MAG_3 believes SharedKey(K_{MAG_3-MN}-, MAG_3, MN) (G_8 **is proved)**

According to S5, P1, Ax1, Ax18 and MP:

S9: MAG_3 believes fresh(K_{MAG_3-MN}) (G_9 **is proved)**

According to P3, Ax1:

S10: MN believes MN received [ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$]K_{LMA_1-MN}

According to S10, P2, Ax3:

S11: MN believes MAG_3 said (ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$)

According to S11, P1, Ax17, Ax19:

S12: MN believes MAG_3 says (ID_{MAG_3}, ID_{LMA_2}, TS_6, $\sigma_{MAG_3\_2}$) (G'_7 **is proved)**

According to P5, S12, Ax1, and Nec:

S13: MN believes PK_δ(MAG_3, σ_{MN_2})

According to S13, P4, Ax5:

S14: MN believes SharedKey(K_{MN-MAG_3}, MAG_3, MN), K_{MAG_3-MN}=F(σ_{MN_2}, $\sigma_{MAG_3\_2}$)

According to P3, Ax1, Ax10:

S15: MN believes MN sees PK_δ(MAG_3, $\sigma_{MAG_3\_2}$)

According to S15, P5, Ax11, Ax12:

S16: MN believes MN sees SharedKey (K_{MN-MAG_3}, MN, MAG_3), K_{MAG_3-MN}= F(σ_{MN_2}, $\sigma_{MAG_3\_2}$)

According to S14, S16, and definition of SharedKey(K-, A, B) :

S17: MN believes SharedKey(K_{MN-MAG_3}-, MN, MAG_3) (G'_8 **is proved)**

According to S4, P1, Ax1, Ax18 and MP:

S18: MN believes fresh(K_{MN-MAG_1}) (G'_9 **is proved)**

C. FURTHER SECURITY ANALYSIS

In this section, we continue to analyze the security features that PAAS satisfies.

1) MUTUAL AUTHENTICATION

The mutual authentication is to guarantee the identity of the other entity during MN's accessing procedure. In initial authentication, MN and MAG can confirm the other entity's identity by verifying the WMS signature. During handover authentication, MN and MAG uses HMAC algorithm to sign and verify the signatures which ensures the legitimacy and authenticity of the other entity.

2) SESSION KEY SECRECY

After authentication protocol is achieved successfully, the confidentiality of the message between MN and MAG is necessary. Thus, it is important that the session key is unknown by the adversary. In other words, during the session key negotiation, adversary cannot get the session key by monitoring the communication between MN and MAG. In PAAS, the session key is generated by DH key exchange approach [34], the adversary couldn't get the session key only by monitoring the key negotiation parameters, which guarantee the session key secrecy.

3) RELIABILITY

During initial access authentication, because there is no way to obtain the legal private key via STR for the adversary, he couldn't generate legal signature and be verified as a legitimate entity. In handover authentication, the shared key between MN and MAG_1 or MAG_2 is only transmitted in the secure tunnel, the adversary does not have chance to attain the shared key and generate HMAC signature to take part in authentication process.

4) RESISTANCE OF MAN-IN-THE-MIDDLE ATTACK

When a man-in-the-middle attack occurs, the adversary can modify, forge or reply the message MN and MAG. Once the message is modified or forged, when the legal verifier authenticates the signature or HMAC, the result will be failure. If reply attack happens, the verifier will find the timestamp is not fresh, which results the authentication is failed.

V. PERFORMANCE ANALYSIS

In this section, we conduct performance analysis by comparing the proposed scheme (PAAS) with HOTA [34], CSS [17]. In most instances, MN executes handover authentication, thus our analysis will be focus on the handover authentication in terms of handover authentication latency, communication overhead, and signaling cost. Before the analysis, the relevant notations, descriptions, and the execution time are shown in Table 2 [35], [36].

A. HANDOVER AUTHENTICATION LATENCY

The handover authentication latency(HL) refers to the time interval from MN sending the first authentication request message to the trust relationship being built between MN and MAG in handover authentication protocol, which contains the computation cost of each entity and the message transfer latency.

TABLE 2. Notation and description in performance analysis.

Notation	Description	Execution time(ms)
T_{PM}	The execution time of point multiplication	0.6
T_{BP}	The execution time of bilinear pairing	4.5
T_{HMAC}	The execute time of HMAC	0.006
T_{Enc}	The execute time of AES-256 encryption	0.00081
T_{Dec}	The execute time of AES-256 decryption	0.00081
D_{A-B}	The latency between entity A and entity B	—

In HOTA, MN first computes the master session key: $msk = Sign\_HMAC\_K_{MN-AS}\{N_{MN}, ID_{MN}, ID_{MAG}\}$ and the authenticator: $Auth = Enc\_K_{MN-MAG}\{ID_{MN}, msk, T, N'_{MN}\}$, where K_{MN-AS} is the sharedkey between MN and authentication server(AS). Then MN sends *Auth* and *TK* to MAG, where $TK = Enc\_K_{TK}\{K_{MN-MAG}, ID_{MN}, T\}$ is generated by AS. After receiving *Auth* and *TK*, MAG uses K_{TK} to decrypt *TK* and sends authentication request: $AuthRes = Enc\_K_{MN-MAG}\{ID_{MN}, N'_{MN}+1\}$ to MN. Finally, MN decrypts *AuthRes* and check $N'_{MN}+1$ to complete the authentication. Thus the handover authentication latency of HOTA is:

$$HL_{HOTA} = T_{HMAC} + 2T_{Enc} + 2T_{Dec} + 2D_{MN-MAG} \quad (1)$$

In CSS, MN computes and sends request message $Req =< SignCrypt\_PK_{AAA}\&SK_{MN}\{ID_{MN}, N\}, H(N) >$ to MAG. After receiving and verifying $H(N)$, MAG transmits $AMR=SignCrypt\_PK_{AAA}\&SK_{MN}\{ID_{MN}, N\}$ to AAA server. Through AMR, AAA server authenticates MN and sends $AMA=SignCrypt\_PK_{MAG}\&PK_{AAA}\{m, N\}$ to MAG. Finally, MAG sends message to authenticate MN. Consequently, the handover authentication latency of CSS is:

$$\begin{aligned} HL_{CSS} &= 2T_{Signcry} + 2T_{Signdec} + 2D_{MN-MAG} \\ &\quad + 2D_{MAG-AAA} \\ &= 16T_{PM} + 4T_{BP} + 2D_{MN-MAG} \\ &\quad + 2D_{MAG-AAA} \end{aligned} \quad (2)$$

During the intra-domain handover authentication of PAAS, MN computes the signature as: $Sign_{MN} = Sign\_HMAC\_K_{MN-MAG_1}\{ID_{MN}, ID_{MAG_1}, TS_3, \sigma_{MN\_2}\}$. Afterwards, $Sign_{MN}$ and the related parameters will be sent to MAG_2. Once receiving MN's signature, MAG_2 verifes $Sign_{MN}$ and computes $Sign_{MAG_2} = Sign\_HMAC\_K_{MN-MAG_1}\{ID_{MAG_2}, TS_4, \sigma_{MAG_2\_2}\}$. Then MAG_2 sends $Sign_{MAG_2}$, ID_{MAG_2}, TS_4, $\sigma_{MAG_2\_2}$ to MN. Finally, MN verifies $Sign_{MAG_2}$ and builds trust relationship between MN and MAG_2. The handover latency of inter-domain handover authentication is similar. Thus, the handover authentication latency of PAAS is:

$$HL_{PAAS} = 4T_{HMAC} + 2D_{MN-MAG} \quad (3)$$

We assume D_{MN-MAG}=20(ms), $D_{MAG-AAA}$=35(ms) [34]. According to (1)-(3), the result of handover authentication latency is shown as Figure.11, and we can get the conclusion that PAAS owns the superiority in handover authentication latency.

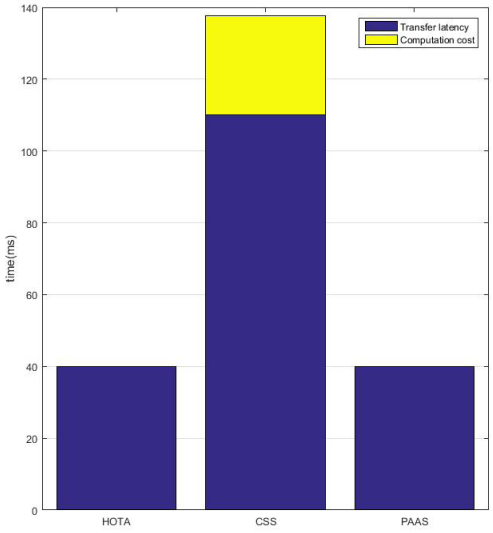


FIGURE 11. Handover authentication latency.

TABLE 3. The size of corresponding parameters.

Parameter	Size(byte)
G_1	128
Z_q^*	20
Timestamp	4
HMAC	16
ID	10
Random number	16

B. COMMUNICATION OVERHEAD

The communication overhead(CO) is the size of total message transmitted during handover authentication. According to [37], [38], the size of corresponding parameters are shown as table 3. HOTA and CSS have no concern of building session key, thus we ignore relevant session key parameters.

In HOTA, MN sends $< Auth, TK >$ to MAG, where $Auth = Enc\_K_{MN-MAG}\{ID_{MN}, msk, T, N'_{MN}\}$, $TK = Enc\_K_{TK}\{K_{MN-MAG}, ID_{MN}, T\}$. After receiving *Auth* and *TK*, MAG sends $AuthRes=Enc\_K_{MN-MAG}\{ID_{MN}, N'_{MN}+1\}$ to MN. The communication overhead of HOTA is:

$$\begin{aligned} CO_{HOTA} &= 3 \times 10 + 2 \times 4 + 4 \times 16(bytes) \\ &= 102(bytes) \end{aligned}$$

In CSS, the communication overhead during handover authentication mainly includes MN's *Areq* and AAA's *AMA*, where $Req =< SignCrypt\_PK_{AAA}\&SK_{MN}\{ID_{MN}, N\}, H(N) >$, since $AMA=SignCrypt\_PK_{MAG}\&PK_{AAA}\{m, N\}$. We ignore the size of message *m*, *m* is the basic configuration information in most cases. Therefore, the communication overhead of CSS is:

$$\begin{aligned} CO_{CSS} &= 3 \times 128 + 6 \times 16 + 2 \times 10(bytes) \\ &= 500(bytes) \end{aligned}$$

In PAAS, MAG_2 first receives the message from MN which includes ID_{MN}, ID_{MAG_1}, TS_3, and

TABLE 4. Communication overhead.

Scheme	Computation(byte)
HOTA	102
CSS	500
PAAS	78

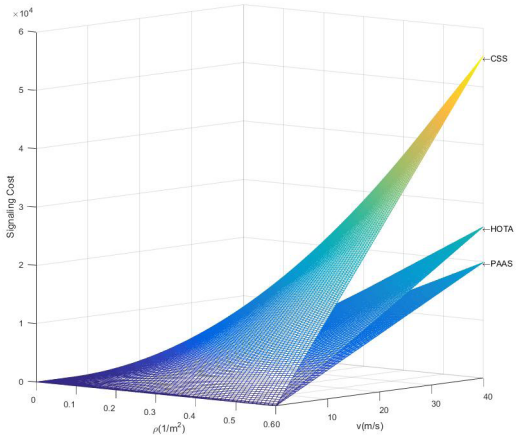


FIGURE 12. Signing cost.

$Sign_{MN} = Sign\_HMAC\_K_{MN-MAG_1}\{ID_{MN}, ID_{MAG_1}, TS_3, \sigma_{MN\_2}\}$. Then MAG_2 sends ID_{MAG_2}, TS_4, and $Sign_{MAG_2} = Sign\_HMAC\_K_{MN-MAG_1}\{ID_{MAG_2}, TS_4, \sigma_{MAG_2\_2}\}$ to MN. Consequently, the communication overhead of PAAS is:

$$\begin{aligned} CO_{PAAS} &= 3 \times 10 + 2 \times 4 + 2 \times 16(bytes) \\ &= 78(bytes) \end{aligned}$$

Compared with HOTA and CSS, the proposed PAAS owns lower communication overhead as shown in Table 4.

C. SIGNALING COST

The signaling cost is defined as the entire amount of authentication signaling costs. We adopt the fluid-flow model [39] to analyze the signaling cost. In this model, it is assumed that all the subnets are circular and of the same size. MN's movement direction is distributed in the range of $(0, 2\pi)$. The crossing rate(R) and signaling cost (SC) can be derived as (4) and (5):

$$R = \frac{\rho v L}{\pi} \tag{4}$$

$$SC = HL \times R \tag{5}$$

Where ρ is the density of MN, v refers to the average velocity of MN, and L means the perimeters of a cell. we assume L=100m, the wired bandwidth is 10Mbps, the wireless bandwidth is 6Mbps. According to Table 2, as the processing time of symmetric key algorithm is about thousands of times faster than the other operations, we ignore the execute time of HMAC, AES-256 encryption and AES-256 decryption.

The results are shown as Figure.12 where we can draw the conclusion that PAAS owns lower signaling cost than the other two schemes.

VI. CONCLUSION

Guaranteeing access authentication and communication security between vehicles and RSUs is the basis for VANETs. Due to shorter signaling overhead and lower handover delay, PMIPv6 can be well combined with VANETs. In this paper, we propose a secure access authentication scheme for PMIPv6 in VANETs(PAAS). Identity-based signature is finely integrated into our hierarchical architecture to achieve distributed mutual authentication between MN and MAG. Security proof under SVO logic is made to prove the robustness of the primary authentication protocols in PAAS. The performance analysis and results demonstrate that PAAS is efficient both for Intra-domain and Inter-domain authentication.

In our further work, we will try to address the privacy-preserving issue during the access authentication of PMIPv6 based on the proposed scheme in this paper.

REFERENCES

[1] Z. Ning *et al.*, "A cooperative quality-aware service access system for social Internet of vehicles," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2017.2764259.

[2] A. Rahim *et al.*, "Vehicular social networks: A survey," *Pervasive Mobile Comput.*, vol. 43, pp. 96–113, Jan. 2017, doi: 10.1016/j.pmcj.2017.12.004.

[3] A. M. Vegni and V. Loscri, "A survey on vehicular social networks," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 4, pp. 2397–2419, 4th Quart., 2015.

[4] C. Perkins, D. Johnson, and J. Arkko, *Mobility Support in IPv6*, document RFC 3775, 2003.

[5] S. Cespedes and X. Shen, "An efficient hybrid HIP-PMIPv6 scheme for seamless Internet access in urban vehicular scenarios," in *Proc. IEEE Global Telecommun. Conf.*, Dec. 2010, pp. 1–5.

[6] H. Soliman, C. Castelluccia, K. El-Malki, and L. Bellier, *Hierarchical Mobile IPv6 (HMIPv6) Mobility Management*, document RFC 5380, 2008.

[7] E. R. Koodli, *Mobile IPv6 Fast Handovers*, document RFC 5568, 2009, pp. 931–934.

[8] W. Hou, Z. Ning, and L. Guo, "Green survivable collaborative edge computing in smart cities," *IEEE Trans. Ind. Informat.*, vol. 14, no. 4, pp. 1594–1605, Apr. 2018.

[9] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, to be published, doi: 10.1109/TII.2018.2816590.

[10] Z. Ning, X. Wang, X. Kong, and W. Hou, "A social-aware group formation framework for information diffusion in narrowband Internet of Things," *IEEE Internet Things J.*, vol. 5, no. 3, pp. 1527–1538, Jun. 2018.

[11] Z. Ning, L. Liu, F. Xia, B. Jedari, I. Lee, and W. Zhang, "CAIS: A copy adjustable incentive scheme in community-based socially aware networking," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 3406–3419, Apr. 2017.

[12] X. Hu *et al.*, "Emotion-aware cognitive system in multi-channel cognitive radio ad hoc networks," *IEEE Commun. Mag.*, vol. 56, no. 4, pp. 180–187, Apr. 2018.

[13] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, *Proxy Mobile IPv6*, document RFC 5213, 2008.

[14] Z. Ning, F. Xia, X. Hu, Z. Chen, and M. S. Obaidat, "Social-oriented adaptive transmission in opportunistic Internet of smartphones," *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 810–820, Apr. 2017.

[15] T. Booth and K. Andersson, "Network security of Internet services: Eliminate DDoS reflection amplification attacks," *J. Internet Services Inf. Secur.*, vol. 5, no. 3, pp. 58–79, 2015.

[16] B. Rashidi and C. Fung, "A survey of Android security threats and defenses," *J. Wireless Mobile Netw., Ubiquitous Comput., Depend. Appl.*, vol. 6, no. 3, pp. 3–35, 2015.

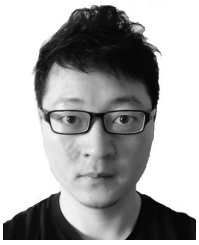
[17] L.-J. Zhang, M. O. Tian-Qinga, and L.-Y. Zhao, "Authentication scheme based on certificateless signcryption in proxy mobile IPv6 network," *Appl. Res. Comput.*, vol. 29, no. 2, pp. 640–643, 2012.

[18] Z. Zhang and G. Cui, "Secure access authentication scheme in mobile IPv6 networks," *Comput. Sci.*, vol. 36, no. 12, pp. 26–31, 2009.

[19] H. C. Zhou, H. K. Zhang, and Y. J. Qin, "An authentication protocol for proxy mobile IPv6," in *Proc. Int. Conf. Mobile Ad-Hoc Sensor Netw. (MSN)*, Wuhan, China, Dec. 2008, pp. 129–136.
[20] H. Kim and J.-H. Lee, "Diffie-hellman key based authentication in proxy mobile IPv6," *Mobile Inf. Syst.*, vol. 6, no. 1, pp. 107–121, 2010.
[21] M.-C. Chuang, J.-F. Lee, and M.-C. Chen, "SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks," *IEEE Syst. J.*, vol. 7, no. 1, pp. 102–113, Mar. 2013.
[22] M. Alizadeh *et al.*, "Cryptanalysis and improvement of 'a secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks,'" *PLoS ONE*, vol. 10, no. 11, pp. 40–48, 2015.
[23] I. You and F.-Y. Leu, "Comments on 'SPAM: A secure password authentication mechanism for seamless handover in proxy mobile IPv6 networks,'" *IEEE Syst. J.*, vol. 12, no. 1, pp. 1038–1041, Mar. 2015.
[24] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Singapore: World Scientific, 1999.
[25] W. Wu, Y. Mu, W. Susilo, J. Seberry, and X. Huang, "Identity-based proxy signature from pairings," in *Proc. Int. Conf. Auton. Trusted Comput.*, 2007, pp. 22–31.
[26] B. Dan and M. Franklin, "Identity-based encryption from the Weil pairing," in *Advances in Cryptology—CRYPTO*. Berlin, Germany: Springer, 2001, pp. 213–229.
[27] B. Waters, "Efficient identity-based encryption without random oracles," in *Advances in Cryptology—EUROCRYPT* (Lecture Notes in Computer Science), vol. 3494. Berlin, Germany: Springer, 2005, pp. 114–127.
[28] H. Yokota, K. Chowdhury, R. Koodli, B. Patil, and F. Xia, *Fast Handovers for Proxy Mobile IPv6*, document RFC 5949, 2010.
[29] P. F. Syverson and P. C. Van Oorschot, "On unifying some cryptographic protocol logics," in *Proc. IEEE Comput. Soc. Symp. Res. Secur. Privacy*, May 1994, pp. 14–28.
[30] M. Burrows, M. Abadi, and R. M. Needham, "A logic of authentication," *Proc. Roy. Soc. London A, Math. Phys. Eng. Sci.*, vol. 426, no. 1871, pp. 233–271, 1989.
[31] A. M. Mathuria, R. Safavi-Naini, and P. R. Nickolas, "On the automation of GNY logic," *Austral. Comput. Sci. Commun.*, vol. 17, no. 1, pp. 370–379, 1995.
[32] M. N. Abadi and M. R. Tuttle, "A semantics for a logic of authentication," in *Proc. ACM Annu. Symp. Princ. Distrib. Comput.*, 1991, pp. 201–216.
[33] P. Van Oorschot, "Extending cryptographic logics of belief to key agreement protocols," in *Proc. ACM Conf. Comput. Commun. Secur. (CCS)*, Fairfax, VA, USA, Nov. 1993, pp. 232–243.
[34] J.-H. Lee and J.-M. Bonnin, "HOTA: Handover optimized ticket-based authentication in network-based mobility management," *Inf. Sci.*, vol. 230, no. 4, pp. 64–77, 2013.
[35] C. Zhang, R. Lu, and X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proc. IEEE Conf. Comput. Commun.*, Apr. 2018, pp. 246–250.
[36] M.-C. Chuang and J.-F. Lee, "SF-PMIPv6: A secure fast handover mechanism for proxy mobile IPv6 networks," *J. Syst. Softw.*, vol. 86, no. 2, pp. 437–448, 2013.
[37] X. Boyen and L. Martin, *Identity-Based Cryptography Standard (IBCS) #1: Supersingular Curve Implementations of the BF and BB1 Cryptosystems*, document RFC 5091, 2007.
[38] C. Adams, P. Cain, D. Pinkas, and R. Zuccherato, *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*, document RFC 3161, 2001.
[39] S. Pack and Y. Choi, "A study on performance of hierarchical mobile IPv6 in IP-based cellular networks," *IEICE Trans. Commun.*, vol. E87-B, no. 3, pp. 462–469, 2004.

TIANHAN GAO received the B.E. degree in computer science and technology, and the M.E. and Ph.D. degrees in computer application technology from Northeastern University, China, in 1999, 2001, and 2006, respectively, and the doctoral tutor qualification in 2016. He has been a Visiting Scholar with the Department of Computer Science, Purdue University, from 2011 to 2012. He joined as a Lecturer with the Software College, Northeastern University, in 2006, where he was promoted as a Professor in 2017. He has authored or co-authored over 50 research publications. His primary research interests are next generation network security, wireless mesh network security, security and privacy in ubiquitous computing, and virtual reality.

XINYANG DENG received the B.E. degree from the Software College, Dalian University of Foreign Languages, in 2014, and the master's degree in software engineering from Northeastern University. His primary research interests are next generation network security, PMIPv6 security, and identity-based cryptography.



YINGBO WANG received the B.A. degree in graphic design from Northeastern University, China, in 2007, and the master's degree in animation making from Chung-Ang University, South Korea, in 2012. From 2008 to 2013, he secured a couple of professional positions as the Director and an Animator, successively from Taktoon Enterprise and Made Contents YAGI Co., South Korea. In 2014, he was well-equipped himself for the honored offer from the Faulty of Software Engineering, Northeastern University, and he has been a Lecturer in subject of digital media technology, specializing in game development, animation production, and virtual reality, since 2014.

XIANGJIE KONG (SM'16) received the B.Sc. and Ph.D. degrees from Zhejiang University, Hangzhou, China. He is currently an Associate Professor with the School of Software, Dalian University of Technology, China. He has served as a Guest Editor for several international journals, and the Workshop Chair or a PC Member for a number of conferences. He has authored or co-authored over 70 scientific papers in international journals and conferences (with over 50 indexed by ISI SCIE). His research interests include human behavior, mobile computing, and computational social science. He is a Senior Member of CCF and a member of ACM.